DIFFUSION GÉNÉRALE

OCDE/GD(95)115

SERIE OCDE
LES PRINCIPES DE BONNES PRATIQUES DE LABORATOIRE
ET LA VERIFICATION DU RESPECT DE CES PRINCIPES
NUMERO 10

DOCUMENT CONSENSUS SUR LES BPL
APPLICATION DES PRINCIPES DE BPL AUX SYSTEMES INFORMATIQUES
MONOGRAPHIE SUR L'ENVIRONNEMENT NO. 116

ORGANISATION DE COOPÉRATION ET DE DÉVELOPPEMENT ÉCONOMIQUES

Paris 1995

SERIE OCDE

LES PRINCIPES DE BONNES PRATIQUES DE LABORATOIRE ET
LA VERIFICATION DU RESPECT DE CES PRINCIPES

Numéro 10

Orientations à l'intention des autorités de vérification en matière de BPL

APPLICATION DES PRINCIPLES DE BPL AUX SYSTEMES INFORMATIQUES

MONOGRAPHIE SUR L'ENVIRONNEMENT NO. 116

Direction de l'Environnement

ORGANISATION DE CO-OPERATION ET DE DEVELOPPEMENT ECONOMIQUES

Paris 1995

AVANT-PROPOS

Dans le cadre du troisième Atelier consensus de l'OCDE sur les bonnes pratiques de laboratoire tenu du 5 au 8 octobre 1992 à Interlaken, Suisse, un groupe d'experts a examiné l'interprétation des principes de BPL appliqués aux systèmes informatiques. Ce groupe d'experts était présidé par M. Theo Helder, représentant l'Autorité néerlandaise de vérification en matière de BPL. Le Rapporteur était M. Bryan Doherty (Président de la Commission informatique de l'Association britannique sur l'assurance qualité dans le secteur de la recherche - BARQA). Les participants au Groupe de travail représentaient pour certains les Autorités nationales de vérification en matière de BPL et, pour d'autres, des laboratoires d'essai des pays suivants : Allemagne, Autriche, Belgique, Danemark, Etats-Unis, Finlande, France, Japon, Pays-Bas, Royaume-Uni et Suisse. Le groupe d'experts a manqué de temps pour pouvoir parvenir à un consensus concernant un document d'orientation détaillé. Il a toutefois mis au point un document intitulé "Concepts relating to Computerised Systems in a GLP Environment", qui énonce les principes généraux et décrit les questions soulevées par chacun. Ce document a été distribué aux pays Membres pour commentaires.

A la lumière des observations formulées, la Commission sur les Bonnes Pratiques de Laboratoire est convenue, à sa cinquième réunion de mars 1993, que d'autres travaux étaient nécessaires et que le groupe de travail devait se réunir une deuxième fois. Le groupe s'est réuni à Paris du 14 au 16 décembre 1994 sous la présidence de M. Helder et avec la participation de M. Doherty en qualité de Rapporteur. Ont assisté à cette réunion des représentants des gouvernements et de l'industrie de l'Allemagne, du Canada, du Danemark, des Etats-Unis, de la France, du Japon, des Pays-Bas, du Royaume-Uni et de la Suède.

Le projet de document consensus préparé par le Groupe d'experts se fonde sur le document issu de la réunion d'Interlaken, les observations formulées par les pays Membres à cette occasion et un document mis au point par un groupe de travail conjoint gouvernement/industrie du Royaume-Uni. Il a par la suite été examiné, modifié et approuvé par la Commission sur les BPL et la Réunion conjointe du Groupe des produits chimiques et du Comité de gestion du Programme spécial sur le contrôle des produits chimiques. Le Comité des politiques d'environnement a ensuite recommandé que le présent document soit mis en diffusion générale sous l'autorité du Secrétaire général.

DOCUMENT CONSENSUS SUR LES BPL : APPLICATION DES PRINCIPES DE BPL AUX SYSTEMES INFORMATIQUES

Ces dernières années, l'utilisation de systèmes informatiques s'est développée dans les installations d'essais pratiquant des essais d'innocuité pour la santé et l'environnement. Ces systèmes informatiques peuvent permettre d'assurer directement ou indirectement la saisie, le traitement, la présentation, et le stockage de données et sont de plus en plus souvent intégrés dans des équipements automatisés. Lorsque ces systèmes informatiques sont associés à l'exécution d'études menées à des fins réglementaires, leur conception, leur validation, leur exploitation et leur maintenance devront être conformes aux Principes de Bonnes Pratiques de Laboratoire de l'OCDE.

Champ d'application

Tous les systèmes informatiques utilisés pour produire, mesurer ou évaluer des données à des fins réglementaires devront être conçus, validés, exploités et gérés dans le respect des Principes de BPL.

Plusieurs systèmes informatiques peuvent assurer diverses fonctions lors de la planification, de l'exécution et de la présentation des résultats des études. Ils peuvent être utilisés pour saisir directement ou indirectement les données enregistrées par des équipements automatisés, exploiter/contrôler les équipements automatisés et enfin traiter, présenter et stocker les données. Les systèmes informatiques utilisés pour ces diverses activités peuvent aller d'instruments d'analyse programmables ou d'un ordinateur personnel, à un système de gestion des informations de laboratoire (LIMS) multifonctions. Les principes de BPL devront être appliqués quel que soit le degré d'intervention de l'ordinateur.

Méthode

Les systèmes informatiques associés à l'exécution d'études réalisées à des fins réglementaires devront être d'une conception appropriée, avoir une capacité adéquate et convenir aux tâches auxquelles ils sont destinés. Des procédures adéquates devront être prévues pour contrôler et gérer ces systèmes qui devront par ailleurs être conçus, validés et exploités en accord avec les Principes de BPL.

L'opération dite "de validation", qui permet de démontrer qu'un système informatique est adapté aux tâches auxquelles il est destiné, joue un rôle déterminant.

La procédure de validation offre de bonnes garanties pour s'assurer qu'un système informatique répond au cahier des charges prévu. La validation doit entrer dans le cadre d'un programme officiel de validation et être exécutée avant la mise en service du système.

Application des Principes de BPL
aux systèmes informatiques

Les considérations ci-après faciliteront l'application des Principes de BPL aux systèmes informatiques décrits ci-dessus :

1. Responsabilités

a) La *direction* de l'installation d'essais assume la responsabilité générale de l'application des Principes de BPL. Il lui appartiendra notamment de nommer un nombre adéquat de personnes suffisamment qualifiées et expérimentées et d'organiser efficacement leur travail, ainsi que de veiller à ce que les installations, les équipements et les procédures de gestion de données répondent aux normes requises.

La direction se charge de veiller à ce que les systèmes informatiques conviennent aux tâches auxquelles ils sont destinés. Elle doit définir des instructions et procédures informatiques pour assurer que les systèmes sont conçus, validés, exploités et entretenus conformément aux Principes de BPL. La direction veillera en outre à ce que ces instructions et procédures soient comprises et observées, et assurera le contrôle effectif de l'application de ces dispositions.

La direction doit également engager du personnel chargé spécifiquement du développement, de la validation, de l'exploitation et de la maintenance des systèmes informatiques. Ce personnel devra être suffisamment qualifié, posséder une bonne expérience et avoir reçu une formation adéquate pour assumer les tâches qui lui sont confiées dans le respect des Principes de BPL.

b) Les *directeurs d'étude* sont responsables, en application des Principes de BPL, de la conduite générale de leurs études. Etant donné que ces études feront souvent appel à des systèmes informatiques, il est indispensable que les directeurs des études soient parfaitement au courant de l'utilisation de tout système informatique intervenant dans les études dont ils sont responsables.

S'agissant des données enregistrées par voie électronique, la responsabilité du directeur d'étude est la même que pour les données enregistrées sur papier et partant, seuls des systèmes validés pourront être utilisés dans les études concernant les BPL.

c) *Personnel*. Tout le personnel utilisant des systèmes informatiques exploitera ces systèmes dans le respect des Principes de BPL. Il appartiendra au personnel chargé de développer, valider, exploiter les systèmes informatiques et d'en assurer la maintenance, d'effectuer ces activités en accord avec les Principes de BPL et les normes techniques reconnues.

d) Les responsabilités en matière d'*assurance qualité* (AQ) des systèmes informatiques seront définies par la direction et décrites dans des instructions et procédures écrites. Le programme d'assurance qualité comprendra des procédures et des pratiques permettant d'assurer que les normes établies sont respectées à toutes les étapes de la validation, de l'exploitation et de la maintenance des systèmes informatiques. Il comprendra en outre des procédures et pratiques pour l'introduction des systèmes achetés et pour l'adaptation de systèmes informatiques aux besoins internes.

Le personnel chargé de l'assurance qualité s'assurera que les systèmes informatiques sont conformes aux BPL et recevra les formations techniques spécialisées que la situation exige. Il connaîtra suffisamment ces systèmes pour pouvoir formuler des avis objectifs ; dans certain cas, il conviendra de nommer des auditeurs qualité.

Le personnel chargé de l'assurance qualité aura accès, en lecture uniquement, aux données stockées dans les systèmes informatiques, pour contrôle.

2. Formation

Pour répondre aux principes de BPL, les installations d'essais doivent employer un personnel qualifié et expérimenté et des programmes de formation détaillés doivent être prévus, comprenant des formations sur poste et, le cas échéant, des cours dispensés à l'extérieur. Les dossiers concernant ces formations seront conservés.

Les dispositions ci-dessus s'appliqueront à tout le personnel participant à l'utilisation des systèmes informatiques.

3. Installations et équipements

Il importera de disposer d'installations et d'équipements propres à assurer la bonne exécution des études en accord avec les Principes de BPL. S'agissant des systèmes informatiques, un certain nombre d'aspects spécifiques seront à prendre en considération :

a) *Installations*

L'emplacement du matériel, des éléments périphériques, des équipements de communication et des supports électroniques sera dûment étudié. Les fortes variations de températures et l'humidité, la poussière, les interférences électromagnétiques et la proximité de câbles à haute tension devront être évités, à moins que l'équipement ne soit expressément prévu pour fonctionner dans de telles conditions.

On étudiera également l'alimentation électrique des équipements informatiques en prévoyant, le cas échéant, une alimentation de secours ou non interruptible pour les systèmes informatiques dont l'arrêt soudain pourrait altérer les résultats d'une étude.

Des équipements adéquats seront prévus pour assurer la sécurité du support électronique d'informations.

b) *Equipement*

i) *Matériel et logiciel*

Un système informatique est défini comme un groupe d'éléments matériels et de logiciels conçu et assemblé pour assurer une fonction ou un groupe de fonctions données.

Le matériel constitue la partie physique du système informatique ; il recouvre l'unité centrale de l'ordinateur et ses périphériques.

Le logiciel est le, ou les, programme(s) nécessaire(s) à l'exploitation du système informatique.

Tous les Principes de BPL applicables aux équipements s'appliquent par conséquent au matériel et au logiciel.

ii) *Communications*

Les communications associées aux systèmes informatiques relèvent grosso modo de deux catégories : elles peuvent relier plusieurs ordinateurs, ou bien des ordinateurs et leurs équipements périphériques.

Toutes les liaisons constituent des sources potentielles d'erreurs et peuvent entraîner la perte ou l'altération de données. Il importera de prévoir des mesures de contrôle adéquates pour assurer la sûreté et l'intégrité des systèmes lors de la conception, de la validation, de l'exploitation et de la maintenance de tout système informatique.

4. Maintenance et reprise après un sinistre

Tous les systèmes informatiques seront installés et entretenus de façon à en assurer le bon fonctionnement permanent.

a) *Maintenance*

Il doit exister des procédures attestées couvrant la maintenance préventive courante et la réparation des défaillances. Ces procédures doivent clairement définir les rôles et responsabilités du personnel concerné. Lorsque ces activités de maintenance ont entraîné une modification du matériel et/ou du logiciel, il pourra être nécessaire de valider à nouveau le système. Tous les problèmes et anomalies détectés pendant l'exploitation du système, ainsi que les mesures correctives appliquées, seront consignés quotidiennement.

b) *Reprise après un sinistre*

Il importe de disposer de procédures décrivant les mesures à prendre en cas de défaillance partielle ou complète d'un système informatique. Ces mesures pourront aller de la redondance planifiée de certains équipements à un retour au système sur support papier. Tous les plans de secours devront être suffisamment détaillés et validés, assurer l'intégrité permanente des données et ne compromettre en aucun cas la réalisation de l'étude. Le personnel participant à l'exécution des études conformément aux Principes de BPL devra être informé de ces plans de secours.

Les procédures de reprise du traitement d'un système informatique seront plus ou moins élaborées selon son importance, mais il sera indispensable de conserver des copies de sauvegarde de tous les logiciels. Si les procédures de reprise exigent de modifier le matériel ou le logiciel, il pourra être nécessaire de valider à nouveau le système.

5. Données

Les principes de BPL définissent les données brutes comme l'ensemble des comptes rendus et des documents originaux de laboratoire, y compris les données entrées directement dans un ordinateur par l'intermédiaire d'une interface d'instrumentation, qui résultent des observations et des travaux originaux réalisés dans le cadre d'une étude, et qui sont nécessaires à la reconstitution et à l'évaluation du rapport sur cette étude.

Les systèmes informatiques exploités conformément aux Principes de BPL peuvent être associés à des données brutes de types très divers : il peut s'agir de supports de données électroniques, de sorties d'ordinateurs ou d'instruments ou encore de microfilms/fiches. Les données brutes seront définies pour chaque système informatique.

Les systèmes informatiques utilisés pour assurer la saisie, le traitement, la communication ou l'archivage de données brutes seront tous conçus pour qu'il soit possible de procéder à une analyse rétrospective pour faire apparaître toutes les modifications des données sans masquer les données de départ. Il devra être possible d'associer chaque modification à la personne qui l'a opérée au moyen de signatures (électroniques) horodatées. Les modifications devront être justifiées.

Lorsque des données brutes sont conservées par voie électronique, il est nécessaire d'assurer les conditions nécessaires à la conservation à long terme du type de données concernés en tenant compte de la durée de vie des systèmes informatiques. En cas de changement de matériel et de logiciel, il devra rester possible d'accéder et de conserver les données brutes sans risquer d'en compromettre l'intégrité.

Les informations auxiliaires, notamment les registres de maintenance et les enregistrements d'étalonnage, nécessaires pour vérifier la validité des données brutes ou permettre la reconstitution d'un processus ou d'une étude doivent être archivées.

Les procédures d'exploitation d'un système informatique doivent aussi décrire des procédures de saisie de données de remplacement à utiliser en cas de défaillance du système. Dans ce cas, toutes les données brutes enregistrées manuellement puis saisies devront être clairement signalées comme telles et conservées comme enregistrements originaux. Les procédures manuelles de sauvegarde serviront à réduire au minimum les risques de perte de données et à assurer que les enregistrements de remplacement sont conservés.

Lorsqu'en raison du vieillissement d'un système, il est nécessaire de transférer des données brutes vers un autre système par voie électronique, on utilisera une procédure attestée dont l'intégrité a été vérifiée. Si un tel transfert n'est pas faisable, les données brutes seront transférées sur un autre support et l'on vérifiera l'exactitude de la copie avant de détruire les fichiers électroniques originaux.

6. Sécurité

Des procédures de sécurité attestées doivent être prévues pour protéger le matériel, le logiciel et les données de toute altération, modification non autorisée ou perte. Dans ce contexte, la sécurité couvre la prévention de l'accès non autorisé ou des modifications du système informatique et des données contenues dans le système. Il conviendra aussi de prendre en considération les risques d'altération des données par des virus ou d'autres agents. Des

mesures de sécurité doivent aussi être prises pour assurer l'intégrité des données en cas de défaillance du système à court et long terme.

a) *Sécurité physique*

Des mesures physiques de sécurité doivent être prévues pour limiter au seul personnel autorisé l'accès au matériel informatique, aux équipements de communication, aux périphériques et aux supports électroniques. S'agissant des équipements qui ne se trouvent pas dans des "salles informatiques" spécialisées (PC et terminaux, par exemple), il importera de prévoir au minimum un contrôle classique à l'accès des installations d'essais. Toutefois, lorsque ces équipements sont situés à distance (éléments portables ou liaisons par modem) d'autres mesures devront être prises.

b) *Sécurité logicielle*

Pour chaque système ou application informatiques, des mesures de sécurité logicielle doivent être prises pour empêcher l'accès non autorisé aux systèmes, applications et données informatiques. Il est indispensable de s'assurer que seuls des versions approuvées et des logiciels validés sont utilisés. La sécurité logicielle peut impliquer de veiller à ce que chaque utilisateur possède une identité unique assortie d'un mot de passe. Toute introduction de données ou logiciels de sources externes devra être contrôlée. Ces contrôles pourront être assurés par le logiciel d'exploitation, par des programmes spécifiques de sécurité, des programmes intégrés aux applications ou par plusieurs de ces moyens.

c) *Intégrité des données*

Etant donné que le maintien de l'intégrité des données est l'un des objectifs premiers des Principes de BPL, il importe que toute personne associée à un système informatique sache qu'il est indispensable de tenir compte des considérations que l'on vient d'évoquer en matière de sécurité. La direction devra veiller à ce que le personnel soit conscient de l'importance de la sécurité des données et connaisse les procédures et fonctions du système qui permettent d'assurer une bonne sécurité ainsi que les conséquences de tout défaut de sécurité. Ces fonctions pourront être une surveillance de routine de l'accès au système, l'application de programmes de vérification des fichiers et la notification des anomalies et/ou tendances.

d) *Sauvegarde*

Il est courant, lorsque l'on utilise des systèmes informatiques, de faire des copies de sauvegarde de tous les logiciels et données pour pouvoir remettre en marche le système après une défaillance susceptible d'en compromettre l'intégrité (détérioration du disque, par exemple). Par conséquent, la copie de sauvegarde doit pouvoir devenir source de données brutes qui seront traitées comme telles.

7. <u>Validation des systèmes informatiques</u>

Les systèmes informatiques doivent être adaptés aux tâches auxquelles ils sont destinés. Il conviendra de prendre en compte les aspects suivants :

a) *Réception*

Les systèmes informatiques doivent être conçus pour répondre aux Principes de BPL et leur introduction doit être préplanifiée. Une documentation adéquate doit montrer que chaque système a été développé sous contrôle et de préférence conformément aux normes de qualité et aux normes techniques reconnues (ISO/9001, par exemple). En outre, il importe de disposer d'éléments concrets montrant que la conformité du système aux critères de réception par l'installation d'essais a été vérifiée avant son entrée en service. Les essais officiels de réception exigent de procéder à des essais selon un plan prédéterminé et de conserver les documents relatifs à toutes les procédures d'essai, les données des essais, leurs résultats, un résumé précis de ces essais et un document de réception officielle.

Dans le cas de systèmes fournis par un vendeur, une grande partie de la documentation créée au cours du développement restera bien souvent chez le vendeur. Dans ce cas, un dossier concernant l'évaluation et/ou la vérification officielles par le vendeur devra être conservé à l'installation d'essais.

b) *Evaluation rétrospective*

Il pourra arriver, pour certains systèmes, que l'impératif de conformité aux Principes de BPL n'ait pas été prévu, ni spécifié. Dans ce type de cas, il conviendra de disposer d'éléments permettant de justifier l'utilisation de ces systèmes ; il s'agira notamment d'une évaluation rétrospective pour évaluer leur adéquation.

Une évaluation rétrospective commence par la collecte de tous les enregistrements rétrospectifs concernant le système informatique. Ces enregistrements sont examinés et un résumé écrit est préparé. Ce résumé d'évaluation rétrospective doit indiquer les éléments disponibles à l'appui d'une validation et ce qu'il faut faire à l'avenir pour que le système informatique soit validé.

c) *Vérification des modifications*

La vérification des modifications est l'approbation et la justification officielles, documents à l'appui, de toute modification du système informatisé pendant sa durée d'exploitation. La vérification des modifications est nécessaire lorsqu'une modification risque d'affecter la validité du système informatique. Les procédures de vérification des modifications doivent être effectives dès lors que le système est opérationnel.

La procédure doit décrire la méthode d'évaluation pour déterminer dans quelle mesure de nouveaux contrôles sont nécessaires pour confirmer la validité du système. Les procédures de vérification des modifications doivent préciser le nom des personnes chargées de déterminer si une vérification des modifications est nécessaire et de l'approuver.

Quelle que soit l'origine de la modification (fournisseur ou développement interne), une information adéquate sera fournie dans le cadre du processus de vérification des modifications. Les procédures de vérification assureront l'intégrité des données.

d) *Mécanisme auxiliaire*

Pour assurer qu'un système informatique reste adapté aux tâches auxquelles il est destiné, des mécanismes auxiliaire seront prévus pour assurer le bon fonctionnement et le bon usage

du système. Il pourra s'agir de dispositions concernant la gestion du système, la formation, la maintenance, l'assistance technique, l'audit et/ou l'évaluation des performances. L'évaluation des performances consiste en un examen officiel effectué périodiquement pour vérifier que le système répond toujours aux critères de performance, en termes notamment de fiabilité, de sensibilité et de capacité.

8. Documentation

Les éléments énumérés ci-après décrivent à titre indicatif la documentation minimum nécessaire au développement, à la validation, à l'exploitation et à la maintenance des systèmes informatiques.

a) *Instructions*

Il doit exister des instructions écrites de la direction couvrant notamment l'acquisition, les caractéristiques, la conception, la validation, l'expérimentation, l'installation, l'exploitation, la maintenance, le personnel responsable, le contrôle, l'audit, la vérification et la mise hors service des systèmes informatisés.

b) *Description des applications*

Pour chaque application, on disposera d'une documentation complète concernant :

* Le nom du logiciel d'application ou le code d'identification ainsi qu'une description claire et détaillée de la vocation de l'application.
* Le matériel (avec les numéros des modèles) sur lequel le logiciel d'application est exploité.
* Le système d'exploitation et les autres logiciels (outils, par exemples) utilisés en liaison avec l'application.
* Le (ou les) langage(s) de programmation de l'application et/ou les outils de bases de données utilisés.
* Les principales fonctions assurées par l'application.
* Une vue générale des types et flux de données/de la conception des bases de données associées à l'application.
* Les structures des fichiers, les messages d'erreur et d'alarme et les algorithmes associés à l'application.
* Les modules du logiciel d'application avec les numéros des versions.
* La configuration et les liaisons entre les modules d'application et avec les équipements et les autres systèmes.

c) *Programme source*

Certains pays de l'OCDE exigent que le programme source du logiciel d'application soit disponible, ou puisse être obtenu, à l'installation d'essais.

d) *Modes opératoires normalisés*

Une grande partie de la documentation concernant l'utilisation des systèmes informatiques se présentera sous forme de Modes opératoires normalisés. Ceux-ci couvriront entre autres :

* Les procédures concernant l'exploitation des systèmes informatiques (matériel/logiciel) et les responsabilités du personnel intéressé.
* Les procédures concernant les mesures de sécurité utilisées pour détecter et prévenir l'accès non autorisé et les modifications des programmes.
* Les procédures et autorisations concernant les modifications des programmes et l'enregistrement des modifications.
* Les procédures et autorisations concernant les modifications des équipements (matériel/logiciel) y compris, le cas échéant, les essais avant emploi.
* Les procédures concernant les essais périodiques pour vérifier le fonctionnement de tout le système ou de certains éléments, et l'enregistrement de ces essais.
* Les procédures concernant la maintenance des systèmes informatiques et de tout autre équipement connexe.
* Les procédures concernant le développement de logiciels et les essais de réception, et l'enregistrement de tous les essais de réception.
* Les procédures de sauvegarde pour toutes les données stockées et les plans de secours en cas de défaillance.
* Les procédures concernant l'archivage et l'extraction de tous les documents, logiciels et données informatiques.
* Les procédures concernant le contrôle et la vérification des systèmes informatiques.

9. Archives

Les Principes de BPL concernant l'archivage des données doivent être appliqués systématiquement pour tous les types de données. Il est donc important que les données informatiques soient stockées avec les mêmes niveaux de contrôle d'accès, d'indexation et de facilité d'extraction que les autres types de données.

Lorsque les données électroniques de deux études et plus sont stockées sur un seul support (disque ou bande), on prévoira un index détaillé.

Il pourra être nécessaire de doter certaines installations de dispositifs de protection du site pour assurer l'intégrité des données informatiques stockées. Si cela nécessite des installations supplémentaires d'archivage, la direction s'attachera à bien définir le personnel responsable de la gestion des archives et à limiter l'accès au seul personnel autorisé. Il importera en outre de mettre en oeuvre des procédures assurant l'intégrité à long terme des données stockées par voie électronique. Si l'accès des données à long terme semble poser des problèmes ou s'il est prévu de mettre certains systèmes informatiques hors service, on établira des procédures pour assurer que les données restent lisibles. Il pourra s'agir par exemple de préparer des sorties sur support papier ou de transférer les données sur un autre système.

Aucune donnée stockée par voie électronique ne pourra être détruite sans autorisation de la direction et sans documentation appropriée. Les autres données auxiliaires concernant les systèmes informatiques telles que les programmes sources et les fichiers de développement, de validation, d'exploitation, de maintenance et de contrôle devront être conservées au moins aussi longtemps que les enregistrements des études associés à ces systèmes.

Définition des termes [1]

Contrôle des modifications : Evaluation permanente sur la base de pièces justificatives des opérations exécutées par un système et de leur modification pour déterminer si une procédure de validation est nécessaire après toute modification du système informatique.

Critères de réception : Critères expressément définis qu'il convient de respecter pour conclure positivement la phase d'essai ou considérer que le système répond au cahier des charges.

Essai de réception : Essai officiel d'un système informatique dans le contexte d'exploitation prévu pour vérifier si tous les critères de réception de l'installation d'essais ont été respectés et si le système peut être accepté pour mise en exploitation.

Logiciel (Application) : Un programme acquis ou développé, adapté ou personnalisé en fonction des conditions de l'installation d'essais, pour assurer les procédures de contrôle, la collecte, le traitement, la présentation et/ou l'archivage des données.

Logiciel (Système d'exploitation) : Programme ou ensemble de programmes ou de sous-programmes commandant le fonctionnement de l'ordinateur. Un système d'exploitation peut assurer des tâches comme l'affectation des ressources, la planification, la gestion des entrées/sorties et la gestion des données.

Matériel : Ensemble des éléments physiques d'un système informatique comprenant l'unité centrale de l'ordinateur et ses périphériques.

Normes techniques reconnues : Normes promulguées par des organismes nationaux ou internationaux de normalisation (ISO, IEEE, ANSI, etc.).

Périphérique : Tout équipement connecté au système ou élément auxiliaire ou distant, tels des imprimantes, modems, terminaux, etc.

Programme source : Programme informatique original rédigé dans un langage lisible par l'homme (langage de programmation) qui est ensuite traduit en langage machine avant de pouvoir être exécuté par l'ordinateur.

Sauvegarde : Dispositions prévues pour récupérer les fichiers de données ou logiciels, relancer le traitement ou utiliser des équipements informatiques de remplacement en cas de défaillance du système ou de sinistre.

Sécurité : Protection du matériel et du logiciel contre l'accès, l'utilisation, la modification, la destruction ou la divulgation accidentels ou délictueux. La sécurité concerne également le personnel, les données, les communications et la protection physique et logicielle des installations informatiques.

---

[1] D'autres termes sont définis dans "Les principes de l'OCDE de Bonnes Pratiques de Laboratoire".

Signature électronique : L’entrée, sous forme d’impulsions magnétiques ou de données informatiques compilées, de tout symbole ou ensemble de symboles, exécutée, adaptée ou autorisée par une personne pour représenter sa signature manuscrite.

Système informatique : Groupe d’éléments de matériel, assorti des logiciels qui s’y rapportent, conçu et assemblé pour assurer une fonction ou un groupe de fonctions données.

Validation d’un système informatique : Opération permettant de démontrer qu’un système informatique est adapté aux tâches auxquelles il est destiné.